

REMARKS

In the Official Action, the Examiner rejected claims 1-55. Accordingly, Applicants respectfully request reconsideration of the present application in view of the remarks presented below.

First Rejection Under 35 U.S.C. § 102

The Examiner rejected claims 1-55 under 35 U.S.C. § 102(b) as being anticipated by Mattison (U.S. Patent No. 5,778,070). Specifically, the Examiner stated:

a. *Referring to claim 1:*

i. Mattison teaches:

- (1) a first section of non-volatile memory

configured to store a BIOS program, the first section of non-volatile memory being reprogrammable [i.e., the BIOS is stored in flash memory to allow for field updates and reprogramming of the BIOS (column 1, lines 56-67). In fact, referring to Figure 2, typically the upper 64 kilobytes in the first megabyte of the original PC architecture is allocated for BIOS (column 7, lines 21-23)]; and

(2) a second section of non-volatile memory operatively coupled to the first section of non-volatile memory, the second section of non-volatile memory being configured to store a boot-block program [i.e., referring to Figure 2, “a boot-block program” is considered to also store in a flash memory 108 (column 5, line 55) and any extensions to the BIOS is contained in a region below the 64 kilobytes allocated to the BIOS, along with any other “program memory”, in which a boot-block program is inherently provided (column 7, lines 23-25)];

(3) the boot-block program having a first validation routine configured to validate the BIOS program stored in the first section of non-volatile memory, and the BIOS program having a second validation routine configured to validate the boot-block program stored in the second section of non-volatile memory [i.e., referring to Figure 3, in block 308, the current program in flash memory 108 is for verifying and/or validating the source and content of the flash memory upgrade program, whereby “a first validation routine configured to validate the BIOS program and a second validation routine configured to validate the

boot-block program” are considered to include in this part of the upgrade program (column 9 lines 38-40)].

...

n. Referring to claims 29 and 42:

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

Applicants respectfully traverse the Examiner’s rejection. Anticipation under section 102 can be found only if a single reference shows exactly what is claimed. *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 U.S.P.Q. 773 (Fed. Cir. 1985). For a prior art reference to anticipate under section 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). To maintain a proper rejection under section 102, a single reference must teach each and every element or step of the rejected claim. *Atlas Powder v. E.I. du Pont*, 750 F.2d 1569 (Fed. Cir. 1984). Accordingly, the prior art reference must show the identical invention in as complete detail as contained in the patent claim to support a *prima facie* case of anticipation. See *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q. 2d 1913, 1920 (Fed. Cir. 1989). As such, Applicants need only to point to a single element not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter.

Additionally, if the Examiner relies on a theory of inherency, the extrinsic evidence must make clear that the missing descriptive matter is *necessarily* present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill in the relevant art. See *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q.2d 1949 (Fed. Cir. 1999). The mere fact that a certain thing *may* result from a given set

of circumstances is not sufficient. *See id.* In relying upon the theory of inherency, the Examiner must provide a basis in fact and/or sound and supportable technical reasoning to support the determination that the allegedly inherent characteristic *necessarily* flows from the teachings of the applied prior art. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (B.P.A.I. 1990). The Examiner, in presenting the inherency argument, bears the evidentiary burden and must adequately satisfy this burden. *See id.* Regarding functional limitations, the Examiner must evaluate and consider the functional limitation, just like any other limitation of the claim, for what it fairly conveys to a person of ordinary skill in the pertinent art in the context in which it is used. *See* M.P.E.P. § 2173.05(g); *In re Swinehart*, 169 U.S.P.Q. 226, 229 (C.C.P.A. 1971); *In re Schreiber*, 44 U.S.P.Q.2d 1429, 1432 (Fed. Cir. 1997). If the Examiner believes the functional limitation to be inherent in the cited reference, then the Examiner “must provide some evidence or scientific reasoning to establish the reasonableness of the examiner’s belief that the functional limitation is an inherent characteristic of the prior art.” *Ex parte Skinner*, 2 U.S.P.Q.2d 1788, 1789 (B.P.A.I. 1986).

The present application is directed to a technique for protecting a computer system and, more particularly, to protecting at least one of a BIOS, boot-block, CMOS, and NVRAM in the computer system. *See* Application, page 2, lines 6-9. Generally, a flashable Basic Input/Output System (BIOS) may include two separate programmable portions to allow the BIOS to be upgraded by flashing without losing operation. *See id.* at page 3, lines 10-20. While this method of flashing the BIOS offers advantages, the ability to upgrade the BIOS creates security risks for the computer system. *See id.* at page 3, line 20 to page 4, line 2. Accordingly, as taught

in the present application, a system may use the BIOS to validate a boot-block and the boot-block to validate the BIOS. *See id.* at page 4, line 14 to page 5, line 8; page 14, lines 18-24. For instance, the boot-block may utilize public/private keys to create digital signatures of the BIOS for validation purposes. *See id.* at Fig. 3; page 15, lines 1-19. In addition, the BIOS may be utilized to validate the boot-block, as well. *See id.* at Fig. 5; page 18, lines 4-24.

This computer protection technique is recited in each of the independent claims 1, 29 and 42. For instance, independent claim 1 recites “the boot-block program having a first validation routine configured to validate the BIOS program” and “the BIOS program having a second validation routine configured to validate the boot-block program.” Similarly, independent claims 29 and 42 recite “validating a BIOS program” and “validating a boot-block program.” To be clear, the independent claims 1, 29, and 42 recite a *boot-block program* and *validating the BIOS and the boot-block program*.

The Mattison reference is directed to a technique for upgrading/downgrading a BIOS from a flash memory. *See Mattison*, col. 2, lines 56-67. To perform this upgrade/downgrade operation, the Mattison reference describes the use of a vendor private key to encrypt an upgrade/downgrade program that is to be installed on a system. *See id.* at col. 3, lines 23-31. The current flash memory verifies the vendor key of the upgrade/downgrade program before an image of the upgrade/downgrade program is loaded into the flash memory. *See id.* at col. 3, lines 32-57. Hence, the Mattison reference is simply directed to a system that upgrades/downgrades an

existing program with a different version of that same program. Importantly, however, the Mattison reference does not disclose the claimed boot-block program, and it certainly does not disclose using a boot-block program to validate BIOS and using BIOS to validate the boot-block program.

In the above-quoted rejection, the Examiner relied upon the Mattison reference and the theory of inherency to reject claims 1-55. While the Examiner did not expressly admit that the Mattison reference does not disclose a “boot-block program,” which is recited in the claims, the Examiner relied upon a specific passage of the Mattison reference, which allegedly discloses this feature inherently. However, despite the Examiner’s reliance upon the Mattison reference, it fails to disclose all the recited features in the present application for at least two reasons. First, the Mattison reference fails to disclose “a boot-block program,” as recited in independent claims 1, 29 and 42. Secondly, the Mattison reference fails to disclose *validating the BIOS and the boot-block program*, which is also recited in independent claims 1, 29, and 42. Hence, Applicants respectfully submit that the Mattison reference fails to disclose, expressly or inherently, all of the subject matter claimed in the present application.

First, a *boot-block program*, as recited in independent claims 1, 29 and 42, is not disclosed or inherently found in the Mattison reference. As the Examiner would certainly agree, the Mattison reference is devoid of any express mention of a *boot-block program*. The reference only describes an upgrade/downgrade program, which is only described as a BIOS program. Because of the lack of express disclosure, the Examiner asserted that a *boot-block program* is inherently provided from a passage, at column 7, lines 23-25, of the Mattison reference. However, the passage relied upon

by the Examiner does not support the Examiner's position. In the cited passage, the reference merely describes how a memory address/window detector 110 operates to control the BIOS memory locations. That is, the reference simply refers to a flash memory upgrade program that interacts with the current program to allow the flash memory program to be upgraded. *See id.* at col. 3, lines 23-36. Thus, the memory address/window detector 110 only allows access to the BIOS program and flash memory 108 when it is being upgraded or downgraded. *See id.* at col. 6, lines 55-col. 7, line 7. Clearly, the passage is simply referencing the BIOS and the BIOS extensions, and does not disclose or infer a *boot-block program*. As a result, the Examiner's assertion does not provide a basis in fact and/or sound or supportable technical reasoning to support the determination that the allegedly inherent characteristic *necessarily* flows from the teachings of the Mattison reference. Therefore, the Examiner has not satisfied the evidentiary burden required by the binding precedences cited above. Accordingly, the "boot-block program," as recited in independent claims 1, 29, and 42, is not inherently found in the Mattison reference.

Secondly, even if the Mattison reference could be construed to inherently disclose a boot-block program, the Mattison reference fails to disclose, inherently or otherwise, *validating the BIOS and the boot-block program*, or more specifically, *validating the BIOS by the boot-block program and the boot-block program by the BIOS*. Again, as noted above, the Examiner relied upon a specific passage to assert that the *boot-block program* is inherently provided within the Mattison reference. Further, in the rejection, the Examiner appears to assert that a second passage, which is located at col. 9, lines 38-40 of the reference, discloses the validation routines. However, the Mattison reference simply refers to a flash memory upgrade/downgrade

program that interacts with a current program to allow the flash memory program to be upgraded. *See* Mattison, col. 3, lines 23-36. To upgrade/downgrade the current program, the Mattison reference discloses the use of vendor private key to encrypt the upgrade program. *See id.* at col. 3, lines 23-31. The Mattison system merely verifies that the vendor's key is from the vendor before the image to the upgrade/downgrade program is loaded into the flash memory. *See id.* at col. 3, lines 32-50. Although this upgrade/downgrade process described in the passage relied upon by the Examiner verifies the replacement program against the current program, the reference does not disclose validating the BIOS *and* the boot-block program, or more specifically, validating the BIOS *by* the boot-block program and the boot-block program *by* the BIOS. Because the reference simply discloses a current program that verifies the vendor type of an upgrade/downgrade program, Mattison fails to disclose validating the BIOS *and* the boot-block program.

Because the Mattison reference fails to disclose all the claimed subject matter, the reference fails to support a *prima facie* case of anticipation. Therefore, Applicants respectfully request withdrawal of the Examiner's rejection and allowance of claims 1-55.

Second Rejection Under 35 U.S.C. § 102

The Examiner rejected claims 1, 29, 30, 36, 42, 43 and 49 under 35 U.S.C. § 102(b) as being anticipated by Davis (U.S. Patent No. 5,844,986). Specifically, the Examiner stated:

- a. Referring to claim 1:
 - i. Davis teaches:

(1) a first section of non-volatile memory configured to store a BIOS program, the first section of non-volatile memory being reprogrammable [i.e., referring to Figure 1, the boot-up program 43 is stored within non-volatile memory 42 (column 3, lines 18-19)]; and

(2) a second section of non-volatile memory operatively coupled to the first section of non-volatile memory, the second section non-volatile memory being configured to store a boot-block program [i.e., referring to Figure 1, “a boot-block program” is considered to also store in a non-volatile memory 42];

(3) the boot-block program having a first validation routine configured to validate the BIOS program stored in the first section of non-volatile memory, and the BIOS program having a second validation routine configured to validate the boot-block program stored in the second section of non-volatile memory [i.e., the primary focus of Davis’ invention, therefore, is to prevent corrupting the BIOS by a computer virus. This is achieved by imposing an authentication and validation procedure before the contents of the BIOS flash memory are modified, whereby “a first validation routine configured to validate the BIOS program and a second validation routine configured to validate the boot-block program” are considered to include in this part of the validation procedure (column 1, lines 63-67.)]

b. Referring to claim 29:

i. Davis teaches:

(1) means for validating a BIOS program stored in a first section of a non-volatile memory [i.e., the authentication and validation are performed by a security processor which contains the BIOS firmware. One example of such a security processor is a cryptographic coprocessor. The cryptographic processor authenticates and validates the BIOS firmware by using secret information such as a digital signature embedded in the BIOS upgrade (column 2, lines 58-63)];

(2) means for validating a boot-block program stored in a second section of non-volatile memory [i.e., referring to Figure 1, the cryptographic processor, that is also for “validating a boot-block program stored in a second section of non-volatile memory”].

...

d. Referring to claim 42:

i. This claim has limitations that is similar to those of claim 29, thus it is rejected with the same rationale applied against claim 29 above.

Applicants respectfully traverse the Examiner's rejection. Again, as noted above, the present application is directed to providing security protection to a computer system. In the present application, the BIOS and boot block are separate programs that provide security protection for the system. The BIOS is a startup routine that allows the system to load and execute subsequent programs, while a boot-block program is a protected segment that may be used to verify the BIOS, NVRAM, and CMOS. *See* Application, page 3, lines 1-6; page 13, line 22 to page 14, line 2. Each of the independent claims includes a boot-block program and a BIOS program. Specifically, independent claim 1 recites "the boot-block program having a first validation routine configured to validate the BIOS program" and "the BIOS program having a second validation routine configured to validate the boot-block program." Similarly, independent claims 29 and 42 recite "validating a BIOS program" and "validating a boot-block program." To be clear, the independent claims 1, 29 and 42 recite a *boot-block program* and *validating the BIOS and the boot-block program*.

The Davis reference is directed to securely updating an executable code through the use of a security processor. *See* Davis, col. 2, lines 10-18. In the Davis reference, authentication and validation are performed a security processor, which contains BIOS firmware. *See id.* at col. 2, lines 58-63. Within the security processor, such as the cryptographic coprocessor 34, a local non-volatile memory 42 may be utilized to store a BIOS program 43, which is also referenced as a *boot-up* program. *See id.* at Fig. 1; col. 3, lines 10-18. The BIOS or *boot-up* program of the Davis reference allows the central processing unit to perform tasks, such as initialization and routine input/output functions, which are utilized in the powering up the system. *See*

id. at col. 1, lines 11-22. Accordingly, the Davis reference describes the use of a cryptographic coprocessor 34 to authenticate the new BIOS that is replacing the current BIOS. *See id.* at col. 3, lines 47-54. As such, the Davis reference simply relates to a method of updating the current BIOS with the new BIOS through the use of a cryptographic coprocessor.

In the above-quoted rejection, the Examiner asserted that the Davis reference disclosed all of the recited features. However, the Davis reference fails to disclose all the recited features in the present application for at least two reasons. First, the Davis reference fails to disclose “a *boot-block* program,” as recited in independent claims 1, 29 and 42. (Emphasis added). Secondly, the Davis reference fails to disclose validating the BIOS *and* the boot-block program, which is also recited in independent claims 1, 29, and 42. Hence, Applicants respectfully submit that the Davis reference fails to disclose all of the subject matter in the present application.

First, the Davis reference does not disclose a “*boot-block* program,” as recited in independent claims 1, 29 and 42. (Emphasis added). Specifically, in the rejection, the Examiner asserted that the “BIOS program” of the claims is equivalent to a *boot-up* program 43, which is also referenced as the BIOS program 43 of the Davis reference. However, the Examiner did not point to or specifically reference any elements that describes or mentions the alleged *boot-block program* in the Davis reference. Indeed, the Davis reference is devoid of any mention of a *boot-block program*. In the Davis reference, the cryptographic coprocessor 34 includes a non-volatile memory 42 that includes a single BIOS program 43. *See* Davis, Fig. 1; col. 3, lines 11-18. Because the Examiner has asserted that the BIOS program 43 is

equivalent to the “BIOS program” of the claim, some other portion of the non-volatile memory 42 must relate to the *boot-block program*. However, the reference fails to describe any other program that may be equivalent to the *boot-block program* being located in the non-volatile memory 42. As a result, the Davis reference, which is strictly directed to upgrading the BIOS program 43, does not any disclose a *boot-block program*. Accordingly, the Davis reference fails to disclose a “boot-block program,” as recited in independent claims 1, 29 and 42.

Secondly, the Davis reference fails to disclose validating the BIOS program *and* the boot-block program, much less, validating the BIOS *by* the boot-block program *and* the boot-block program *by* the BIOS. As noted above, the authentication and validation in the Davis reference are performed by the security processor, which contains the BIOS firmware. *See* Davis, col. 2, lines 58-59. This is done to validate the BIOS upgrade through the use of a digital signature embedded in the BIOS upgrade. *See id.* at col. 2, lines 59-63. The cryptographic coprocessor 34, which is the security processor, performs the appropriate authentication by utilizing the public/private key cryptography to verify the BIOS provider before upgrading the current BIOS. *See id.* at col. 3, line 57-col. 4, line 7. However, the Davis reference clearly does not disclose using a boot-block program to validate the BIOS upgrade. Furthermore, the Davis reference does not disclose validating a boot-block program *and* a BIOS, much less, a BIOS *validating* a boot-block program *and* a boot-block program *validating* a BIOS.

Because the Davis reference fails to disclose all the claimed subject matter, the reference fails to support a *prima facie* case of anticipation. Therefore, Applicants

respectfully request withdrawal of the Examiner's rejection and allowance of claims 1, 29, 30, 36, 42, 43 and 49.

Rejection Under 35 U.S.C. § 103

The Examiner rejected claims 11, 20, 31, 37, 44 and 50 under 35 U.S.C. § 103(a) as being unpatentable over Mattison (U.S. Patent No. 5,778,070) in view of Davis et al. (U.S. Patent No. 6,401,208). Applicants respectfully traverse this rejection.

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Accordingly, to establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985). When prior art references require a selected combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gained from the invention itself, i.e., something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination. *Uniroyal Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 5 U.S.P.Q.2d 1434 (Fed. Cir. 1988).

Each of the claims 11, 20, 31, 37, 44 and 50 depend from independent base claims that are clearly patentable over the Mattison reference, as discussed above. To reject these claims, the Examiner asserted that the Mattison reference discloses all the claimed features except the subject matter of these dependent claims. In an attempt to remedy these deficiencies, the Examiner relied upon the Davis reference. The Davis reference describes a cryptographic device that authenticates software code before allowing the processor to execute the software. *See* Davis, col. 1, lines 63-67. In the Davis reference, a storage device 170 contains BIOS code 180, a digital certificate 181, and a digital signature 182 that utilizes a private key of the BIOS vendor. *See id.* at col. 3, lines 32-40. Further, a cryptographic device 410, which includes an internal memory 525 having firmware 526, is used to initialize and authenticate the storage element 170. *See id.* at col. 4, lines 41-58. The firmware 526 and a root certification key are initially pre-programmed into the internal memory 525 of the cryptographic device 410 during the manufacture process. *See id.* at col. 5, lines 9-13. As such, the Davis reference simply describes validating a BIOS code against a cryptographic device and nothing else. Because the reference simply discloses a single authentication of the BIOS code by a cryptographic device, the reference fails to disclose a *boot-block program*, much less, validating the BIOS *and* the boot-block program, as recited in claims 1, 29 and 42. As such, the Davis reference fails to cure the deficiencies of the Mattison reference. Accordingly, in view of the remarks set forth above, Applicants respectfully submit that the proposed combination does not render the claimed subject matter obvious.

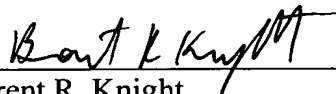
Because the Examiner has failed to show that the cited references disclose all of the claimed subject matter, the Examiner has failed to establish a *prima facie* case of obviousness. Therefore, Applicants respectfully request withdrawal of the rejection and allowance of claims 11, 20, 31, 37, 44 and 50.

Conclusion

In view of the remarks set forth above, Applicants respectfully request allowance of the pending claims 1-55. If the Examiner believes that a telephonic interview will help speed this application toward issuance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Date: 06/04/2004



Brent R. Knight
Reg. No. 54,226
(281) 970-4545

Correspondence Address:

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 8527-2400